

**Notice of References Cited**

Application/Control No.

09/390,362

Applicant(s)/Patent Under  
Reexamination  
VANSTONE ET AL.

Examiner

Odaiche T Akpati

Art Unit

2131

Page 1 of 1

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name          | Classification |
|---|---|--|-----------------|---------------|----------------|
|   | A | US-5915024                                       | 06-1999         | Kitaori et al | 380/25         |
|   | B | US-  |                 |               |                |
|   | C | US-  |                 |               |                |
|   | D | US-  |                 |               |                |
|   | E | US-  |                 |               |                |
|   | F | US-  |                 |               |                |
|   | G | US-  |                 |               |                |
|   | H | US-  |                 |               |                |
|   | I | US-  |                 |               |                |
|   | J | US-  |                 |               |                |
|   | K | US-  |                 |               |                |
|   | L | US-  |                 |               |                |
|   | M | US-  |                 |               |                |

**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name     | Classification |
|---|---|--|-----------------|---------|----------|----------------|
|   | N | EP-0639907-A1                                    | 02-1995         | Europe  | Nyberg   | H04L 9/32      |
|   | O | EP-0918274-A2                                    | 05-1999         | Europe  | McCollom | G06F 1/00      |
|   | P |  |                 |         |          |                |
|   | Q |  |                 |         |          |                |
|   | R |  |                 |         |          |                |
|   | S |  |                 |         |          |                |
|   | T |  |                 |         |          |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)  |
|---|---|--|
|   | U | ISO/IEC FCD 9796-1: Digital Signature Schemes giving message recovery. Part 1: Mechanisms using redundancy." ISO/IEC JTC 1/SC27, July 7, 1999, No. 2352, Berlin, Germany.  |
|   | V | CORON, J.-S., NACCACHE, D., STERN, J.P., "On the Security of RSA Padding", Advances in Cryptology CRYPTO'99, Proceedings of the 19 <sup>th</sup> Annual International Cryptology Conference, August 19, 1999, Pages 1-18, Springer-Verlag, Berlin, Germany |
|   | W | Handbook of Applied Cryptography, by Menezes, Alfred J., Oorschot Paul C. van, Vanstone, Scott A., pg. 363.  |
|   | X |  |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)

Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.